OSSERVATORIO
DI POLITICA INTERNAZIONALE

# Criticità nell'architettura istituzionale a protezione dello spazio cibernetico nazionale

n. 117 – marzo 2016

Approfondimenti

A cura dello IAI (Istituto Affari Internazionale)

**OSSERVATORIO DI POLITICA INTERNAZIONALE**

**Istituto Affari Internazionali**
**(IAI)**

# Criticità nell'architettura istituzionale a protezione dello spazio cibernetico nazionale

*di Tommaso De Zan*, junior researcher *presso*
*l'Area Sicurezza e Difesa dello IAI*

marzo 2016

# I N D I C E

## *Executive Summary*

Il tema della sicurezza cibernetica è sempre più al centro del dibattito politico sia italiano che internazionale, in ragione della sua grande rilevanza per la sicurezza, l'economia e la resilienza della società contemporanea. **La presente ricerca ha l'obiettivo di individuare problematiche e criticità all'interno del nostro sistema di sicurezza cibernetica nazionale**. Qual è l'architettura istituzionale preposta alla protezione dello spazio cibernetico nazionale? Chi si trova a capo di questo assetto istituzionale? Quali sono le istituzioni o gli organi che hanno un ruolo all'interno di questa struttura? Quali sono le criticità e le possibili soluzioni alternative?

**Lo studio è partito dall'analisi della legislazione vigente e dai documenti ufficiali in materia di sicurezza cibernetica**. Successivamente, sono state costruite delle ipotesi sui possibili elementi di criticità dell'architettura, poi verificate attraverso interviste strutturate e semi-strutturate con esperti provenienti dalle istituzioni, dal giornalismo, dall'accademia e dal settore privato.

Il quadro che ne esce non è sicuramente di facile analisi. Da una parte è forse meno problematico di quello che si poteva supporre dalla lettura della legislazione e dei documenti ufficiali, ma risulta più complesso per altri aspetti. Teoricamente, la Presidenza del Consiglio dei Ministri è a capo dell'architettura nazionale, ma di fatto la protezione della sicurezza cibernetica nazionale ha avuto un carattere fortemente compartecipato.

Questo non costituisce di per sé una debolezza del sistema, ma può indurre a nutrire dei dubbi su chi debba avere la responsabilità della politica di sicurezza cibernetica nazionale. Sarebbero quindi auspicabili, in un'ottica riformatrice, misure tendenti alla centralizzazione del sistema, sebbene non vi sia convergenza su un tipo di evoluzione piuttosto che un altro. A puro titolo di esempio, sono stati citati fra le possibili alternative la nomina di un'autorità delegata, la creazione di un'agenzia oppure di un'autorità amministrativa indipendente.

L'analisi della legislazione e dei documenti ufficiali sembrava evidenziare una sovrapposizione di funzioni, ruoli e competenze degli attori dell'architettura istituzionale. L'analisi ha però dimostrato che la sovrapposizione di ruoli e competenze tra organismi ed amministrazioni, pur se effettivamente presente in alcuni casi specifici, è stata attenuata da una divisione dei compiti "sul campo" e dalla comunicazione fra i vari organi in situazioni operative. Anche una diversa maturazione, nel corso degli anni, degli organi preposti alla prevenzione, al contrasto e alla

gestione del rischio ha indotto gli attori del sistema ad agire pragmaticamente sulla base delle capacità a disposizione. Queste sovrapposizioni, anche se solo parziali, potrebbero comunque essere superate attraverso l'accorpamento dei ruoli, dei compiti e della capacità in un'unica struttura, che dovrebbe avere nella sicurezza la sua missione principale.

**Una struttura unificata probabilmente renderebbe anche più semplice ed efficiente l'allocazione delle risorse**. Questa esigenza risulta tanto più pressante se si considera che le risorse disponibili per la protezione cibernetica sono ridotte rispetto a quelle previste da altri paesi. Infine, una razionalizzazione degli organismi in un'unica struttura dovrebbe facilitare il reclutamento e l'addestramento di personale dotato delle adeguate competenze tecniche, fattore cruciale in un campo così complesso come quello della sicurezza cibernetica.

## Introduzione

Se il tema della sicurezza cibernetica fosse una trasmissione televisiva, recentemente si sarebbe registrata un'impennata negli ascolti. **Nel dicembre 2015 il Governo ha annunciato lo stanziamento di 150 milioni di euro nella nuova legge di stabilità 2016** per il "*potenziamento degli interventi e delle dotazioni strumentali in materia di protezione cibernetica e di sicurezza informatica nazionali*"[1].

I nuovi fondi hanno chiaramente suscitato l'interesse dei molti attori istituzionali preposti alla sicurezza cibernetica e aperto un dibattito su chi e in quale misura debba poter disporre di queste risorse[2].

Il dibattito che si è creato in Italia ha fatto emergere questioni importanti che vale la pena affrontare in maniera sistematica e scientifica, al di là di considerazioni politiche: qual è l'architettura istituzionale preposta alla protezione dello spazio cibernetico nazionale? Chi si trova a capo di questo assetto istituzionale? Quali sono le istituzioni o gli organi che hanno un ruolo all'interno di questa struttura? Ci sono delle criticità nell'attuale architettura istituzionale? Quali sono le possibili soluzioni alternative?

Per rispondere a queste domande, **la presente ricerca è partita dall'analisi della legislazione vigente e dai documenti ufficiali in materia di sicurezza cibernetica**. Successivamente, sono state costruite delle ipotesi sui possibili elementi di criticità dell'architettura italiana.

Queste ipotesi sono state poi verificate attraverso delle interviste strutturate e semi-strutturate con esperti di sicurezza cibernetica provenienti dalle istituzioni, dal giornalismo, dall'accademia e dal settore privato[3]. I risultati di questa ricerca, ai paragrafi 2.3 e 2.4, presentano le reali criticità dell'organizzazione italiana per la protezione dello spazio cibernetico e

---

[1] "Legge di Stabilità: salta sconto Ires nel 2016" in Ansa, 13 dicembre 2015, http://www.ansa.it/sito/notizie/economia/2015/12/13/legge-di-stabilita-salta-sconto-ires-nel-2016_ec8cab6d-2adc-4d02-bf7c-c03c0b9f37f9.html.

[2] "Cyber security, ecco i fondi a disposizione di Renzi e Carrai" in *Formiche*, 20 gennaio 2016, http://formiche.net/2016/01/20/cyber-renzi-carrai-legge-stabilita/.

[3] Si ringraziano per le interviste fornite l'Ente nazionale per l'assistenza al volo (Enav), gli esponenti del Parlamento e delle amministrazioni che vi hanno partecipato in maniera anonima, oltre all'Ufficio del Consigliere militare presso la Presidenza del Consiglio dei Ministri per il supporto fornito nel corso dell'indagine. Si ringraziano anche Roberto Baldoni (Laboratorio Nazionale di cyber security), Raoul Chiesa (Security Brokers), Luisa Franchina (Associazione Italiana esperti in Infrastrutture Critiche), Stefano Mele (Carnelutti Studio Legale Associato e Istituto Italiano di Studi Strategici "Niccolò Machiavelli"), Paolo Messa (Airpress e Formiche) e Pierluigi Paganini (Bit4Id).

offrono, nelle conclusioni, degli spunti di riflessione sulle possibili soluzioni.

## L'architettura istituzionale italiana per la sicurezza cibernetica e le sue problematiche

L'architettura istituzionale italiana è delineata nel Decreto del Presidente del Consiglio dei Ministri (Dpcm) del 24 gennaio 2013. Tuttavia, per avere un panorama completo in materia è necessario analizzare anche altri documenti chiave: il Quadro Strategico nazionale per la sicurezza dello spazio cibernetico, il Piano Nazionale per la protezione cibernetica e la sicurezza informatica (dicembre 2013) ed infine la Direttiva presidenziale del 1 agosto 2015. Rilevanti informazioni sono poi contenute nei documenti di sicurezza nazionale allegati alla Relazione sulla politica dell'informazione per la sicurezza al Parlamento.

### *L'assetto istituzionale italiano: sintesi dei documenti ufficiali*

Il **decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013** definisce l'architettura istituzionale preposta alla protezione cibernetica nazionale, indicando ruoli e compiti dei soggetti individuati, nonché i meccanismi per la prevenzione dei rischi e per la gestione di crisi di natura informatica[4]. Il dpcm individua tre livelli d'azione: il primo di indirizzo politico e coordinamento strategico, un secondo di supporto e con funzioni di raccordo tra le varie amministrazioni e il terzo di gestione delle crisi[5].

Il decreto ravvisa la necessità di un **forte collegamento fra la politica dell'informazione per la sicurezza e gli altri ambiti di azione**, e concentra "*in un organismo interministeriale l'organo d'indirizzo politico e di coordinamento strategico nel campo della sicurezza cibernetica*"[6]. Tale organismo è il Comitato Interministeriale per la Sicurezza della Repubblica (Cisr), composto dal Presidente del Consiglio dei Ministri, l'Autorità delegata, e i ministri degli Affari Esteri e della Cooperazione internazionale (Maeci), dell'Interno, della Difesa, della Giustizia,

[4] Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale. (13A02504) (GU Serie Generale n.66 del 19-3-2013), decreto del Presidente del Consiglio dei Ministri, 24 gennaio 2013 http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.
[5] *Ibidem.*
[6] *Ibidem.*

dell'Economia e delle Finanze (Mef) e dello Sviluppo economico (Mise)[7]. Spetta al Direttore del Dipartimento delle Informazioni per la Sicurezza (Dis) la funzione di segretario del comitato. Il Cisr si può avvalere dell'organismo collegiale permanente (il c.d. "Cisr tecnico"), istituito presso Dis.

Per quel che riguarda la gestione delle crisi di natura cibernetica, il **decreto prevede la costituzione permanente di un Nucleo per la sicurezza cibernetica** (Nsc) presso l'Ufficio del Consigliere militare del Presidente del Consiglio dei Ministri, e di un "**Tavolo interministeriale di crisi cibernetica**" (come configurazione specifica del Nucleo Interministeriale Situazione e Pianificazione, Nisp), per un'ulteriore e specifica esigenza di coordinamento.

Secondo il decreto:

a) Il Presidente del Consiglio adotta il Quadro Strategico nazionale su proposta del Cisr; adotta il Piano Nazionale per la protezione cibernetica su deliberazione del Cisr e infine emana le direttive per l'attuazione del Piano Nazionale;

b) Il Cisr propone al Presidente l'adozione del Quadro Strategico e delibera il Piano Nazionale; esprime parere sulle direttive del Presidente; sorveglia l'attuazione del Piano Nazionale, approva le linee di indirizzo per favorire la collaborazione fra gli attori istituzionali e stabilisce gli obbiettivi in materia di protezione cibernetica nazionale. Alle riunioni del Cisr che hanno come oggetto la sicurezza cibernetica prende parte, senza diritto di voto, il Consigliere militare;

c) "L'Organismo collegiale di coordinamento" (il c.d. "Cisr tecnico") supporta il Cisr nelle sue attività ed è presieduto dal Direttore del Dis. Partecipano al Cisr tecnico i direttori dell'Agenzia informazioni e sicurezza esterna (Aise), dell'Agenzia informazioni e sicurezza interna (Aisi) e i dirigenti di vertice dei ministeri Cisr, in aggiunta al Consigliere nilitare. Il Cisr tecnico prepara le riunioni del Cisr in materia di sicurezza cibernetica e verifica l'implementazione del Piano Nazionale; inoltre formula le attività di analisi delle minacce, del riconoscimento delle vulnerabilità e l'adozione di migliori pratiche ("*best practices*").

[7] "Cisr", Sistema di informazione per la Sicurezza della Repubblica, https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/comitato-interministeriale-per-la-sicurezza-della-repubblica-Cisr.html.

d) Il Nsc, istituito presso l'Ufficio del Consigliere militare, collega i vari attori dell'architettura istituzionale e gestisce le situazioni di crisi cibernetica. È composto dai rappresentanti di Dis, Aise, Aisi, Maeci, Interno, Difesa, Mise, Mef, del Dipartimento Protezione Civile e dell'Agenzia per l'Italia Digitale (Agid)[8]. Si riunisce almeno una volta al mese. L'Nsc è coinvolto nelle attività di preparazione e prevenzione di eventuali crisi cibernetiche: promuove la pianificazione di esercitazioni di crisi cibernetica; raccoglie le informazioni circa le violazioni (o tentativi di) della sicurezza di reti e servizi; acquisisce informazioni in merito ad incidenti informatici dalle amministrazioni competenti e costituisce il punto di riferimento nazionale per i rapporti con Onu, Nato e Ue, tenendo conto delle competenze delle altre amministrazioni. Durante una crisi riceve le segnalazioni riguardanti un attacco informatico e attiva, se necessario, il Nisp, quale Tavolo interministeriale di crisi cibernetica.

e) Il **Tavolo interministeriale di crisi cibernetica è presieduto dal Consigliere militare** ed è composta dai rappresentanti delle amministrazioni indicate nel Dpcm 5 maggio 2010 più un rappresentante del Mise e dell'Agid[9]. In caso di crisi cibernetica, assicura il coordinamento delle attività di reazione e stabilizzazione di competenza delle diverse amministrazioni, e si avvale del **Cert nazionale** (Cert-N) per gli aspetti tecnici.

f) Operatori privati che gestiscono reti pubbliche di comunicazione o servizi di comunicazione elettronica e le infrastrutture critiche di rilievo nazionale ed europeo, (comprese quelle indicate dal Decreto del Ministro dell'Interno del 9 gennaio 2008), devono informare il Nsc di significative violazioni alla sicurezza dei propri sistemi informatici; adottare le migliori pratiche nel campo della sicurezza

[8] Rispetto alla composizione del Cisr, manca un rappresentante del Ministero della Giustizia.

[9] Il NISP è composto da due rappresentanti del Maeci, dell'Interno e della Difesa, da un rappresentante del Mef, del Ministero della Salute, del Dipartimento Protezione Civile, del Dis, dell'Aisi, dell'Aise e del Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, quale rappresentante, anche, della Commissione di cui all'art. 6, comma 4, nonché da un dirigente dell'Ufficio stampa e del Portavoce del Presidente, da uno dell'Ufficio del Consigliere diplomatico e da uno dell'Ufficio del Consigliere militare del Presidente del Consiglio dei Ministri.
http://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=5&art.versione=1&art.codiceRedazionale=10A07594&art.dataPubblicazioneGazzetta=2010-06-17&art.idGruppo=0&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=0

informatica, fornire informazioni al Dis consentendone l'accesso alle banche dati e collaborare alla gestione delle crisi cibernetiche[10].

L'Italia si è dotata di un **Quadro strategico nazionale** e di un **Piano nazionale per la sicurezza cibernetica** nel dicembre 2013, dopo l'entrata in vigore del decreto del 24 gennaio dello stesso anno. Il Quadro Strategico è stato elaborato dal Tavolo tecnico Cyber (Ttc), istituito nell'aprile 2013 quale emanazione del Cisr tecnico e presieduto dal Dis. Fanno parte del Ttc i rappresentanti della sicurezza cibernetica dei sei ministeri Cisr (Maeci, Interno, Difesa, Giustizia, Mef, Mise), dell'Agid, dell'Aise, dell'Aisi e del Nsc[11].

Il Quadro strategico nazionale mira "*ad accrescere la capacità di risposta del Paese alle presenti e future sfide riguardanti lo spazio cibernetico, […] nella consapevolezza che la protezione dello spazio cibernetico è un processo più che un fine*"[12]. Oltretutto, "*al fine di garantire al Paese i benefici sociali ed economici derivanti da uno spazio cibernetico sicuro ed allo scopo di rafforzare le capacità nazionali di prevenzione, reazione e ripristino*", con "*un ruolo di raccordo e impulso del Cisr*" vengono presentati sei indirizzi strategici e undici indirizzi operativi[13].

Nell'allegato del Quadro strategico vengono altresì specificati i ruoli e i compiti dei vari attori dell'architettura cibernetica nazionale:

a) **Agenzia per l'Italia digitale**: sottoposta ai poteri di indirizzo e vigilanza del Presidente del Consiglio dei Ministri, o del Ministro da lui delegato, realizza gli obiettivi dell'agenda digitale italiana nel contesto dell'agenda digitale europea. Detta indirizzi, regole tecniche, e linee guida in materia di sicurezza informatica e di uniformità dei linguaggi, delle procedure e degli standard per assicurare l'interoperabilità dei sistemi della P.A. e tra questi e i sistemi dell'Unione europea; garantisce la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro interconnessione; gestisce il Cert della Pubblica Amministrazione

[10] Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, cit.
[11] Non siede al Ttc il Dipartimento di Protezione Civile.
[12] Quadro strategico nazionale per la sicurezza dello spazio cibernetico, Presidenza del Consiglio dei Ministri, dicembre 2013, p. 10, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf.
[13] *Ibidem*, p. 19.

(Cert-Pa), che garantisce la sicurezza dei sistemi informativi della P.A. e coopera con il Cert-N e il Cert Difesa[14].

b) **Dis** (inclusi Aise e Aisi): il Dis, coadiuvato dalle Agenzie, raccoglie le informazioni finalizzate alla protezione dello spazio cibernetico nazionale e si occupa della formulazione di analisi, valutazioni e previsioni della minaccia cibernetica. Definisce le misure di sicurezza informatica delle infrastrutture che trattano informazioni classificate e/o coperte dal segreto di Stato. È consentito al Dis e alle agenzie l'accesso agli archivi informatici delle pubbliche amministrazioni e dei soggetti erogatori di servizi pubblici secondo le modalità previste dal Dpcm n.4/2009. Il Dis redige un documento di sicurezza nazionale concernente la protezione delle infrastrutture critiche, materiali e immateriali e la sicurezza informatica, da allegare alla relazione annuale al Parlamento[15].

c) Il **Maeci**: coordina la partecipazione e l'impegno italiano nei diversi fora internazionali in materia di sicurezza cibernetica; negozia le intese internazionali sul tema e collabora per il recepimento nell'ordinamento interno degli obblighi assunti a livello internazionale; il Cert-Maeci è accreditato presso il Cert-Pa[16].

d) **Ministero dell'Interno**: attraverso il Dipartimento della Pubblica Sicurezza, previene e contrasta il crimine informatico. La Polizia Postale e delle Comunicazioni garantisce l'integrità e la funzionalità delle reti informatiche, la sicurezza dei servizi di comunicazione, il contrasto a crimini online, inclusi la pedopornografia, gli illeciti riguardanti i mezzi di pagamento e i servizi di "home banking" e le attività terroristiche condotte tramite mezzi informatici; il Centro Nazionale Anticrimine per la Protezione delle Infrastrutture Critiche (Cnaipic) protegge le infrastrutture critiche informatizzate e le strutture strategiche per il paese[17].

e) **Ministero della Difesa**: definisce e coordina la politica militare nello spazio cibernetico; conduce operazioni nello spazio cibernetico per contrastare le minacce contro le reti e i sistemi della Difesa sul territorio nazionale; "contribuisce al flusso informativo a supporto delle operazioni cibernetiche delle F.A. oltre i confini nazionali"; concorre a prevenire e contrastare le attività terroristiche online contro i sistemi e le reti delle Forze Armate; contribuisce alle

[14] *Ibidem*, pp. 29-30.
[15] *Ibidem*, pp. 31-32.
[16] *Ibidem*, p. 33.
[17] *Ibidem*, 34.

operazioni di gestione di crisi cibernetica assieme al Cert Nazionale e al *Nato Computer Incident Response Capability* (Ncirc) della Nato; partecipa alle attività di contrasto di azioni mirate contro i sistemi di comunicazione e informazione strategica per gli interessi nazionali[18].

f) **Ministero dell'Economia e delle Finanze**: al suo interno sono costituite le Unità locali di sicurezza (Uls)[19], Uls Mef/Sogei e Uls df/Sogei, accreditate presso il Cert-Pa. Inoltre, la Guardia di Finanza svolge compiti di prevenzione e repressione dei crimini informatici di carattere economico (frodi)[20].

g) **Ministero dello Sviluppo economico**: è l'Autorità nazionale in materia di sicurezza delle reti di comunicazione elettronica, la quale individua le misure tecniche e ne verifica la loro implementazione; riceve dagli operatori le segnalazioni di incidenti significativi per poi trasmetterle alla Commissione Europea e all'Enisa[21]; gestisce il Cert-N[22]; rappresenta l'Italia all'Enisa tramite il Direttore dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Iscom)[23].

**Il Piano Nazionale è un piano d'azione per l'applicazione dei sei indirizzi strategici e degli undici indirizzi operativi esposti nel Quadro strategico**. Proprio come il Quadro strategico, il Piano è stato elaborato dal Ttc. La sua applicazione verrà valutata attraverso determinati criteri elaborati dallo stesso Ttc[24].

---

[18] *Ibidem*, p. 35.

[19] Pur semplificando, le ULS, come i CERT, possono essere definiti come gli organi che gestiscono a livello operativo gli incidenti informatici.

[20] Quadro strategico nazionale per la sicurezza dello spazio cibernetico, cit, p. 36.

[21] L'Enisa è l'agenzia dell'Unione Europea per la sicurezza dei sistemi e delle informazioni.

[22] Secondo quanto previsto dalla RFC 2350, il CERT-N supporta cittadini e imprese attraverso azioni nella prevenzione e nel coordinamento in risposta ad eventi cibernetici su vasta scala. Esso fornisce informazioni su potenziali minacce, facilitare la risposta ad un incidente informatico e dare supporto al Nsc in caso di crisi cibernetica. Il CERT-N offre i suoi servizi anche ai principali operatori privati gestori di infrastrutture critiche informatizzate e cerca di ottenere i suoi obbiettivi con una piattaforma di "condivisione delle informazioni". Il CERT-N coordina anche la risposta agli eventi nazionali fino alla loro risoluzione. Computer Emergency Response Team CERT Nazionale Italia – (IT-CERT), Profilo RFC 2350, https://www.certnazionale.it/content/uploads/2015/10/IT-CERT_RFC_2350_1_7_IT.txt.

[23] L'Iscom "opera nell'ambito del Ministero dello Sviluppo Economico in qualità di organo tecnico-scientifico. La sua attività, rivolta specificamente verso le aziende operanti nel settore ICT, le Amministrazioni pubbliche e l'utenza, riguarda fondamentalmente la normazione, la sperimentazione e la ricerca di base e applicata, la formazione e l'istruzione specializzata nel campo delle telecomunicazioni", "Chi è Iscom", http://www.isticom.it/index.php/presentazione.

[24] Piano Nazione per la protezione cibernetica e la sicurezza informatica, Presidenza del Consiglio dei Ministri, p. 8: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf.

Di estrema rilevanza per la valutazione dell'architettura nazionale per la sicurezza dello spazio cibernetico sono poi i documenti di sicurezza nazionale allegati alla Relazione sulla politica dell'informazione per la sicurezza del 2013 e 2014.

Nella relazione del 2013 si riporta che il Ttc ha contribuito allo sviluppo dell'architettura istituzionale e nella "messa a sistema" delle sue varie componenti[25]. Il Ttc ha promosso al suo interno l'adozione di una matrice per la verifica dell'applicazione del Piano e il miglioramento delle capacità tecnologiche del paese in materia di sicurezza informatica.

Il Ttc si è impegnato anche nel favorire l'avvio di importanti elementi dell'architettura, quali il Cert-N, il Cert-Pa, il Nsc e l'istituzione del "Tavolo Tecnico Imprese" (Tti). A quest'ultimo partecipano circa dieci soggetti, ossia quelli considerati, secondo la dicitura del Dpcm del 24 gennaio 2013, quali gestori di servizi di pubblica utilità e attori privati di rilevanza strategica, e con i quali il Dis ha sottoscritto delle apposite convenzioni[26].

**La relazione del 2014** ha evidenziato ancora una volta l'importante apporto del Ttc nell'implementazione del Piano nazionale e ha evidenziato i progressi effettuai nella messa a regime di Nsc, Cert-N e Cert-Pa. Oltre a ciò, il Dis ha sottoscritto un accordo di collaborazione con il Consorzio Interuniversitario Nazionale per l'Informatica (Cini) e ha favorito la creazione di un Laboratorio Nazionale di Cyber Security al suo interno. Sempre il Dis, ha potenziato il rapporto con il Ministero della Difesa e dell'Interno, in particolare con il Cnaipic, per rendere più sistematico e regolare lo scambio di informazioni e il sostegno alle indagini riguardanti attacchi informatici e di analisi. Infine, il Dis ha realizzato una "**Piattaforma di Cyber Collaboration**" con gli operatori facenti parte del Tti: la "Piattaforma" consiste essenzialmente in un tavolo che si riunisce periodicamente presso il Dis.

**La direttiva del Presidente del Consiglio del 1 agosto 2015** costituisce l'ultimo documento ufficiale riguardante la strategia nazionale cibernetica e la sua applicazione. La direttiva riguarda i ministri del Cisr, l'Autorità delegata, i direttori dell'Agid, del Dis, dell'Aise, dell'Aisi, il Consigliere Militare, e infine, una novità rispetto al passato, il Ministro per

[25] Sistema di informazione per la sicurezza della Repubblica, Relazione sulla politica dell'informazione per la sicurezza 2014, febbraio 2015, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/relazione-2013.pdf.
[26] Sistema di informazione per la sicurezza della Repubblica, Relazione sulla politica dell'informazione per la sicurezza 2013, febbraio 2014, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/relazione-2013.pdf.

la Semplificazione e la Pubblica Amministrazione. Sentito il parere del Cisr, il Presidente del Consiglio chiede un'accelerazione nella realizzazione degli indirizzi strategici e operativi fissati nel Quadro Strategico e nel Piano Nazionale, con particolare riferimento al:

1) potenziamento delle capacità di reazione ad eventi cibernetici[27]
2) coordinamento istituzionale[28]
3) partenariato pubblico-privato[29]
4) ricerca nazionale con università e centri di ricerca privati[30]
5) cooperazione internazionale

Tra le disposizioni finali, la direttiva chiede all'Autorità delegata e al Direttore del Dis di seguire l'attuazione delle linee d'azione, "per gli aspetti di competenza", e di riferire al Presidente ogni sei mesi[31].

### *Ipotesi sugli elementi di criticità dell'assetto istituzionale italiano*

La valutazione dei documenti ufficiali permette di ravvisare una serie di elementi di criticità che possono essere sintetizzati in due macro argomenti: la problematica delle scelte di indirizzo politico e strategico in materia di protezione cibernetica (di seguito, punti 1-2-3) e quella delle possibili sovrapposizioni fra i vari attori dell'architettura istituzionale (di seguito, punti da 4 fino a 11).

Le ipotesi presentate di seguito sono poi state verificate attraverso una serie di interviste, i cui risultati sono riassunti nel paragrafo successivo.

Come ricordato anche dal Quadro wtrategico, "*al vertice dell'architettura si colloca Il Presidente del Consiglio dei Ministri*"[32]. Il Presidente è coadiuvato dal Cisr, che propone il Quadro strategico e

[27] L'Agid è chiamata presentare standard minimi di prevenzione e reazione ad eventi cibernetici. Nsc, Cert-N e Cert-Pa devono potenziare la propria operatività, allineandosi agli standard internazionali.
[28] Viene richiesta la predisposizione di una rete di comunicazione classificata per evitare disfunzioni durante l'evento di crisi, garantendo lo scambio di informazioni fra amministrazioni, i Cert e il Nsc.
[29] Viene richiesto di potenziare la sensibilizzazione alla minaccia cibernetica anche ad operatori privati che, se attaccati, potrebbe avere delle conseguenze sul sistema-paese. Gli attori verranno definiti dal Cisr tecnico.
[30] Soprattutto per quel che riguarda lo sviluppo di strumenti di rilevamento di intrusioni nei sistemi informatici.
[31] Direttiva del 1 agosto 2015 del Presidente del Consiglio dei Ministri, https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html.
[32] Quadro strategico nazionale per la sicurezza dello spazio cibernetico, cit., p. 26.

delibera il Piano nazionale, in linea con lo spirito del Dpcm del 24 gennaio 2013, che concentra "*in un organismo interministeriale l'organo di indirizzo politico e di coordinamento strategico nel campo della sicurezza cibernetica*", e con quanto affermato nel Quadro strategico, che conferma al Cisr "*un ruolo di raccordo e impulso*"[33], nonostante poi il Presidente del Consiglio si possa avvalere di direttive per favorire l'attuazione del Piano Nazionale.

Sembrerebbe quindi configurarsi, di fatto, **una condivisione del ruolo di vertice tra la figura del Presidente del Consiglio e il Cisr**. In quest'ottica, e considerato l'ordinamento costituzionale italiano, in cui il Presidente del Consiglio è rispetto ai ministri un *primus inter pares*, sembra che la formulazione e l'implementazione della strategia cibernetica nazionale abbia avuto un carattere fortemente collegiale e che quindi non si sia adottata una logica verticistica nell'assunzione delle decisioni.

**Il carattere collegiale del processo decisionale**, pur non costituendo un elemento di criticità in sé, **potrebbe indurre a dubitare circa la provenienza, e quindi la responsabilità, dell'indirizzo politico in materia di sicurezza cibernetica**. Inoltre, esso potrebbe rallentare l'implementazione degli obbiettivi della strategia, dato il numero maggiore di attori che devono dare il proprio consenso nel processo.

Secondo il Dpcm del 24 gennaio 2013, **il Nsc dovrebbe svolgere funzioni di raccordo tra le diverse parti dell'architettura nazionale**. Secondo i documenti di sicurezza nazionale allegati alla Relazione al Parlamento, l'organo che più di ogni altro supporta la "messa a sistema" dell'architettura è invece l'emanazione del Cisr Tecnico, ovvero il Ttc. Una chiara distinzione di competenze fra i due organi sembrerebbe necessaria, anche nella valutazione della "catena di comando", soprattutto in condizioni di operatività quotidiana (ossia ad esclusione di casi di crisi cibernetica) per via della loro diversa composizione[34] e delle diverse figure istituzionali alla guida[35].

**Per quanto riguarda il Ttc, non è facile valutare se il Dis abbia avuto un ruolo centrale**, nella messa a sistema delle parti dell'architettura. Il Ttc, va ricordato, opera presso il Dis ed è emanazione del Cisr Tecnico, presieduto dal Direttore generale del Dis. Il ruolo chiave del Dis sembra oltretutto evincersi dalla direttiva del Presidente del Consiglio del 1 agosto 2015, che chiede all'Autorità delegata e al Direttore del Dis di "*seguire*

[33] *Ibidem*, p. 18.
[34] All'interno del Nsc non è rappresentato il Ministero della Giustizia, sostituito da un rappresentante del Dipartimento della Protezione civile.
[35] Il Nsc è presieduto dal Consigliere militare, mentre il Ttc dal Dis.

*l'attuazione delle linee d'azione indicate, per gli aspetti di competenza*" e di riferire al Presidente con cadenza semestrale. Tuttavia, è ipotizzabile che altre istituzioni potrebbero opporre resistenza ad affidare l'attuazione della strategia di protezione cibernetica ad una struttura (Dis) che ha nella raccolta informativa la sua funzione principale. Inoltre, uno squilibrio di poteri tra istituzioni potrebbe costituire fonte di tensione, soprattutto riguardo all'influenza sull'allocazione di risorse non originariamente previste.

Secondo il Dpcm 24 gennaio 2013, nel rispetto delle competenze dei vari ministeri, **il Nsc dovrebbe essere il punto di contatto per le relazioni con Ue, Nato e Onu nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi**, "fermo restando le specifiche competenze" del Mise, del Maeci, dell'Interno e della Difesa. Proprio per via delle specifiche competenze dei suddetti ministeri, i quali hanno intavolato da tempo rapporti rispettivamente con l'Enisa (Ue), il Ncirc (Nato) e l'Onu, in caso di crisi cibernetica potrebbe risultare problematico capire la gestione del flusso di informazioni fra organi nazionali e internazionali.

Secondo il **Quadro strategico, la protezione delle infrastrutture critiche è affidata alla Polizia Postale e delle comunicazioni**, nella fattispecie al Cnaipic. Secondo quanto previsto dalla Rfc 2350, anche il Cert-N offre i propri servizi (azioni nella prevenzione e nel coordinamento in risposta ad eventi cibernetici) a "un gruppo chiuso e ristretto, del quale possono fare parte i principali operatori privati gestori di infrastrutture critiche informatizzate"[36]. Secondo il Quadro strategico, anche la Difesa concorre alla prevenzione e al contrasto degli attacchi contro i sistemi di comunicazione e informazione di rilevanza strategica per gli interessi nazionali.

Dato il decreto del Ministro dell'Interno del 2008 "*Individuazione delle infrastrutture critiche informatiche d'interesse nazionale*", che identifica come infrastrutture critiche informatizzate "Ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute", anche l'Agid, che garantisce la sicurezza dei sistemi informativi della P.A., sembra possa avere un ruolo nella protezione delle infrastrutture critiche.

Secondo il Dpcm del 24 gennaio 2013, **gli operatori privati** (coloro che gestiscono reti pubbliche di comunicazione o servizi di comunicazione

[36] Computer Emergency Response Team CERT Nazionale Italia – (IT-CERT), Profilo RFC 2350, https://www.certnazionale.it/content/uploads/2015/10/IT-CERT_RFC_2350_1_7_IT.txt.

elettronica, nonché le infrastrutture critiche) **dovrebbero comunicare al Nsc significativi attacchi contro i propri sistemi, effettuando una segnalazione** che probabilmente dovrebbe essere diretta anche al Cert-N e al Cnaipic. Secondo il Dpcm del 24 gennaio del 2013, anche il Nsc acquisisce informazioni da operatori privati che forniscono reti pubbliche di comunicazione o infrastrutture critiche in merito ad incidenti informatici significativi.

Il Dis ha costituito il Tti a cui partecipano dieci soggetti considerati gestori di pubblica attività e attori privati di rilevanza strategica e con i quali ha sottoscritto delle convenzioni ed elaborato una "Piattaforma di Cyber Collaboration" per un rapido scambio di informazioni. Anche il Cert-N sembra offrire ai principali operatori privati gestori di infrastrutture critiche informatizzate informazioni su potenziali minacce attraverso la condivisione di una piattaforma delle informazioni[37].

**Il Cnaipic previene e contrasta azioni terroristiche *online***, attività che potrebbe accavallarsi con quella del comparto di intelligence che si occupa della formulazione, valutazione e previsione della minaccia, inclusa quella di matrice terroristica.

**Il Cert-N supporta cittadini e imprese** attraverso azioni nella prevenzione e nel coordinamento in risposta ad eventi cibernetici, potenzialmente andando a sovrapporsi alle attività della Polizia Postale[38].

**La Polizia postale contrasta gli illeciti** concernenti i mezzi di pagamento e i servizi di "home banking", potenzialmente andando a sovrapporsi con le attività della Guardia di Finanza.

[37] Ibidem.
[38] In questo caso una discriminante potrebbe essere data dall'entità dell'incidente informatico (il Cert-N si dovrebbe occupare di incidenti "su vasta scala").

## Alla prova dei fatti: problemi reali e non nella protezione dello spazio cibernetico

Queste ipotesi sui possibili elementi di criticità del sistema istituzionale italiano sono state verificate attraverso una serie di interviste con esperti di sicurezza delle informazioni in Italia. Gli intervistati sono rappresentanti delle Istituzioni, del giornalismo, dell'accademia e del settore privato[39]. Più interlocutori hanno sottolineato come il dpcm del 24 gennaio 2013 sia il prodotto di un periodo storico particolare, che ha costretto gli ideatori del decreto ad agire in tempi ristretti.

L'attuale architettura nazionale è stata generalmente giudicata come "rivedibile" e "migliorabile". In materia di *governance* si sono espressi dei nuovi dubbi, non rilevabili dall'analisi dei documenti ufficiali, sull'efficienza del processo decisionale in seno al Nsc durante una crisi. Le interviste hanno poi confermato alcune sovrapposizioni rilevate in precedenza, anche se in generale si può affermare che alcune di esse non si siano realizzate completamente, o che le amministrazioni si siano organizzate per evitarle.

**In tema di struttura della *governance*** vi è una generale tendenza fra gli esperti a considerare la Presidenza del Consiglio quale vertice dell'architettura nazionale, anche se fra gli organi citati compaiono il Dis, il Cisr, il Nsc, e il Cert-N. Questo sembra confermare come, anche fra gli esperti, ci possano essere dei dubbi circa la provenienza dell'indirizzo politico in materia di protezione dello spazio cibernetico. Nonostante l'identificazione della Presidenza del Consiglio quale vertice dell'architettura nazionale, è stato confermato come il processo decisionale si sia realizzato in maniera partecipata, attraverso il meccanismo del consenso all'interno del Ttc.

Questa modalità decisionale non è stata valutata come particolarmente farraginosa o suscettibile di allungare il processo di implementazione della strategia di protezione cibernetica anche se, per una valutazione più completa, occorrerà attendere la pubblicazione della "matrice di verifica" nel documento di sicurezza nazionale allegato alla Relazione al parlamento del 2015.

I vari esperti intervistati non hanno riscontrato una sovrapposizione nelle competenze fra il Ttc o il Ncs in quanto i due organi hanno funzioni

[39] La verifica delle ipotesi circa gli elementi di criticità dell'assetto istituzionale italiano risente inevitabilmente della mancata partecipazione alle interviste da parte di alcune amministrazioni facenti parte dell'architettura nazionale. Le interviste sono state condotte attraverso questionari strutturati e semi-strutturati.

complementari e diverse: il **Ttc quale organo di formulazione** e implementazione di politiche per la protezione dello spazio cibernetico, **il Nsc come tavolo per la pianificazione di esercitazioni e/o l'attivazione delle procedure di allertamento**.

Fra gli interlocutori è emerso un certo consenso nel considerare il Dis quale istituzione di riferimento nell'azione di raccordo per la formulazione e l'implementazione della strategia all'interno del Ttc[40]. Ciononostante, questo ruolo maggiore del Dis non ha generato malcontenti all'interno dell'organo, proprio per via del processo decisionale basato sul consenso che impedisce una supremazia di un'istituzione sulle altre. Inoltre, si è affermato che un maggiore ruolo da parte di un'istituzione non sia in grado di influenzare l'allocazione di fondi non originariamente previsti, anche in questo caso per il sistema collegiale alla base dell'assunzione delle decisioni.

In merito alla possibilità che, durante una crisi, ci sia sovrapposizione fra il Nsc da una parte e Cert-N, Cert Difesa e Maeci dall'altra, i colloqui hanno sottolineato come questa situazione in realtà non si verifichi poiché il Nsc si compone dei rappresentati proprio di queste istituzioni, i quali dovrebbero dialogare con i rispettivi partner internazionali durante un'emergenza informatica. All'interno del Nsc un'unità di allertamento sembra garantisca il flusso delle informazioni fra le varie amministrazioni in seguito alla raccolta di segnalazioni di attacchi.

Sebbene si fosse rilevata inizialmente una possibile contrapposizione con il Cert-N, la maggior parte degli intervistati ha nella sua quasi totalità considerato il Cnaipic come l'istituzione a cui è affidata la protezione delle infrastrutture critiche. Contrariamente a quanto ci si potesse aspettare, il Cert-N è stato citato solo marginalmente fra le risposte. Nella pratica l'attività dei due organi è stata complementare. Il Cert-N ha compiti di condivisione delle informazioni ("info-sharing") sia in fase preventiva che reattiva, e fornisce un coordinamento di tipo tecnico alla crisi (come ad esempio indicatori di compromissioni delle reti), mentre il Cnaipic ha funzioni di contrasto e di polizia giudiziaria. Si può dunque affermare che nella realtà i due organi operano su piani diversi.

Il Cert-N è stata la risposta più fornita alla domanda su quale organo gli operatori privati, secondo la definizione del Dpcm gennaio 2013[41], dovrebbero contattare per comunicare incidenti informatici alle proprie reti o sistemi. Solo marginalmente sono stati citati il Ncs e il Cnaipic. Secondo

[40] Tra le risposte fornite, compaiono, anche se in misura minore, il Nsc e il Cisr.

[41] Gli operatori privati che forniscono reti pubbliche e di comunicazione o servizi di comunicazione elettronica, nonché le infrastrutture critiche rilevanti a livello nazionale europeo.

il Dpcm questi operatori dovrebbero comunicare anche al Ncs violazioni significative. Come rilevato in precedenza, tuttavia, la natura stessa del Nsc in quanto tavolo fa sì che le comunicazioni ad una delle istituzioni rappresentate al Nsc costituisca di fatto una segnalazione all'organo stesso. Come espresso al punto cinque, le diverse responsabilità e tipo di operatività fra Cert-N e Cnaipic portano i due organi ad operare su piani differenti per cui l'efficace gestione di una crisi passa inevitabilmente per un coordinamento dei due organi, ed eventualmente, il Nsc. Nonostante la sovrapposizione fra di essi sembra non esserci, ciò non toglie che la molteplicità degli attori possa rendere difficoltosa da parte di operatori privati l'identificazione dell'organo da contattare, per lo meno in una fase iniziale di situazione di crisi.

Le interviste hanno confermato la similitudine tra la "Piattaforma di Cyber Collaboration" portata avanti dal Dis con i gestori di pubblica attività e gli attori privati di rilevanza strategica e la piattaforma gestita dal Cert-N, offerta ai principali operatori privati gestori di infrastrutture critiche informatizzate[42].

Le risposte da parte di esperti hanno confermato la sovrapposizione nelle attività di prevenzione e di raccolta informativa fatta da Cnaipic e Intelligence. Questa sovrapposizione è però attenuata da uno scambio di informazioni costante fra i due soggetti, a maggior ragione a fronte della stipulazione di un protocollo d'intesa in fase di finalizzazione[43].

La possibile dicotomia fra Cnaipic e Cert-N nelle attività di prevenzione e coordinamento in risposta ad incidenti informatici a supporto di cittadini e imprese è stata attenuata dalle interviste per via del diverso ruolo fra i due organi, di contrasto e repressione del primo, di scambio delle informazioni preventivo e reattivo a crisi per quel che riguarda il secondo.

Le interviste hanno parzialmente confermato possibili azioni parallele in ambito di contrasto di crimini di natura economico/finanziaria fra Polizia Postale e Guardia di Finanza.

[42] Computer Emergency Response Team CERT Nazionale Italia – (IT-CERT), Profilo RFC 2350, https://www.certnazionale.it/content/uploads/2015/10/IT-CERT_RFC_2350_1_7_IT.txt.

[43] Quadro strategico nazionale per la sicurezza dello spazio cibernetico, Presidenza del Consiglio dei Ministri, dicembre 2013, p. 10, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf.

**Altre (rilevanti) criticità non riscontrate dall'analisi dalle fonti legislative o dai documenti ufficiali**

Nel corso delle interviste sono state rilevate altre problematiche che, a detta di molti esperti, ri**schiano di indebolire il sistema a protezione dello spazio cibernetico** forse ancora maggiormente rispetto ad una catena di comando non perfettamente chiara o a delle possibili sovrapposizioni tra istituzioni ed organismi, parziali o complete che siano. In particolare si sono rilevati:

1) ***Possibili rallentamenti nel processo decisionale in sede di Nsc***: benché il meccanismo di prevenzione e preparazione ad eventuali crisi di natura cibernetica sembra sia stato "oleato" grazie ad esercitazioni congiunte fra i vari attori (anche privati)[44], alcuni interlocutori hanno suggerito la possibilità di velocizzare il processo decisionale convocando al tavolo Nsc esclusivamente coloro che rappresentano strutture "operative", ovvero che dispongono delle risorse tecniche necessarie per la valutazione, il contrasto e la mitigazione della minaccia. Ad attenuare i possibili problemi derivanti dal coordinamento della molteplicità di attori in seno al Nsc, sembra vi sia stata una certa "sensibilità istituzionale" fra le varie amministrazioni nel permettere a chi disponeva degli strumenti tecnici adeguati di poter operare in indipendenza a seconda delle condizioni. Fino ad oggi, va tuttavia rilevato, non si sono mai verificate situazioni tali da costringere la convocazione del Nisp come tavolo interministeriale di crisi cibernetica. E' quindi possibile che condizioni di particolare urgenza, non verificatesi finora, possano far risaltare le lentezze di un processo giudicato come perfettibile. Oltre a ciò, alcuni hanno rilevato nel passaggio di responsabilità fra Nsc a Nisp un ulteriore possibile elemento di rallentamento in caso di crisi particolarmente gravi che, per la natura stessa della minaccia cibernetica, richiederebbe l'assunzione di decisioni in tempo reale.

*2)* ***Maggiore operatività a livello tecnico***: questa esigenza è emersa soprattutto nella valutazione delle operazioni quotidiane, le quali richiedono delle competenze specialistiche in ambito ingegneristico-informatico, in attività di monitoraggio e/o prevenzione, contrasto e/o repressione e di gestione del rischio. Ad oggi si stima che il numero di operatori afferenti alle strutture che si dovrebbero occupare di queste fasi, Cert-N, Cert-Pa e Polizia Postale sia attorno

[44] "Cyber Italy 2015: esercitazione nazionale sulla sicurezza informatica", in Iscom, 3 dicembre 2015, http://www.isticom.it/index.php/archivio-sicurezza-ict/8-articoli/379-cyber-2015.

alla cinquantina, benché si debbano considerare anche gli operatori del comparto intelligence e della Difesa, di cui non abbiamo a disposizione i dati. Alcuni degli intervistati si sono spinti fino a dichiarare che nessuno dei Cert italiani funzioni secondo gli standard che sarebbe necessari, dato il basso numero di addetti e la qualità dei dati su cui essi poggiano la loro azione.

3) ***Competenza ed expertise***: il tema delle competenze è emerso più volte nel corso dello svolgimento dell'indagine ed è ascrivibile sia alla questione della responsabilità della linea politica e di indirizzo, che al tema dell'operatività a livello tecnico. C'è una forte convergenza nell'affermare che la linea politica/strategica debba avvalersi di figure competenti in ambito tecnologico e informatico e disporre degli strumenti necessari per poter dare impulso all'implementazione dell'attuale piano. In questo senso, durante le interviste sono stati proposti vari criteri di valutazione per l'individuazione di esperti, fra cui esperienze comprovabili nel settore della sicurezza delle informazioni, pubblicazioni di carattere scientifico, posizioni di rilievo in associazioni o organizzazioni di categoria e altri fattori più soggettivi come connessioni dirette in settori rilevanti della sicurezza cibernetica e la stima da parte di colleghi internazionali. Comprovate capacità non dovrebbero caratterizzare solo i vertici del sistema, ma anche il personale tecnico preposto alla gestione quotidiana di incidenti informatici, il quale dovrebbe poter ricevere una formazione secondo standard di livello internazionale.

4) *Maggiori risorse:* la questione delle risorse da allocare alla sicurezza dello spazio cibernetico nazionale è stata più volte registrata come un elemento di forte negatività nel presente contesto. In chiave comparativa le risorse previste nella più recente Legge di Stabilità (circa 150 milioni di euro) impallidiscono di fronte alle risorse allocate su base annua in altri paesi europei come Inghilterra (circa 2,5 miliardi di euro)[45] o Francia (circa 1 miliardo di euro)[46].

[45] "Chancellor's speech to GCHQ on cyber security" in GovUK, 17 novembre 2015.
[46] "France to invest 1 billion euros to update cyber defences", in Reuters, 7 febbraio 2015.

## Conclusioni

La ricerca ha avuto come obiettivo l'individuazione di problematiche e criticità all'interno del nostro sistema di sicurezza cibernetica nazionale: sulla base dell'analisi dei documenti ufficiali, sono state costruite delle ipotesi che sono poi state verificate attraverso delle interviste. **Alcune di queste criticità sono state smentite, alcune confermate, altre attenuate, mentre altre sono emerse**.

**Il quadro che ne esce non è sicuramente di facile analisi**: da una parte è forse meno problematico di quello che si poteva supporre dalla lettura della legislazione e dei documenti ufficiali, ma risulta più complesso per altri aspetti. Tralasciando le problematiche che sono state perentoriamente smentite dalla realtà dei fatti, faremo delle brevi considerazioni sulle criticità più importanti che invece sono state confermate, attenuate o quelle che sono emerse.

**Sembra effettivamente sussistere l'idea che, teoricamente, a capo dell'architettura nazionale vi sia la Presidenza del Consiglio dei Ministri**, quando di fatto, per una questione di ordinamento costituzionale italiano e per le dinamiche che hanno portato alla formulazione e all'implementazione della strategia cibernetica nazionale, la protezione della sicurezza cibernetica nazionale ha avuto un carattere fortemente compartecipato.

Come espresso in precedenza, **questo non costituisce di per sé una debolezza del sistema, ma può indurre a nutrire dei dubbi su chi debba avere la responsabilità della politica di sicurezza cibernetica nazionale**. In un'intervista è stato fatto notare che "il coordinamento è nulla senza direzione, ovvero capacità di incidere sulle decisioni da intraprendere". In un'ottica riformatrice, si è giudicata in maniera tendenzialmente favorevole una centralizzazione del sistema, sebbene non vi sia stata convergenza su un tipo di evoluzione piuttosto che un altro. A puro titolo di esempio, sono stati citati fra le possibili alternative la nomina di un'autorità delegata, la creazione di un agenzia oppure di un'autorità amministrativa indipendente.

**Una maggiore centralizzazione è valutata positivamente soprattutto se in grado di dare impulso alla formulazione, all'implementazione e alla valutazione/controllo di politiche in quest'ambito**, nel rispetto delle competenze degli organi coinvolti nell'architettura nazionale e avvalendosi delle rispettive competenze. Come esercizio teorico, un importante passo avanti deriverebbe dalla comprensione di come, tenuto conto di aspetti strutturali derivanti dall'assetto costituzionale e amministrativo nazionale, sia possibile promuovere una maggiore centralizzare del nostro assetto

istituzionale. Legato a questo aspetto, si dovrebbe valutare anche come rendere più rapido, il processo decisionale durante una crisi.

L'analisi della legislazione e dei documenti ufficiali sembrava certificare in maniera inequivocabile la sovrapposizione di funzioni, ruoli e competenze degli attori della nostra architettura istituzionale. Tale sovrapposizione appariva così grave ed endemica che la raffigurazione grafica più azzeccata dell'architettura complessiva, considerando solo la legislazione e i documenti ufficiali, sarebbe stata simile ad un gomitolo.

La disamina ha però dimostrato che la sovrapposizione di ruoli e competenze tra organismi ed amministrazioni, pur se effettivamente presente in alcuni casi specifici, è stata attenuata da una divisione dei compiti "sul campo" e dalla comunicazione fra i vari organi in situazioni operative. Anche una diversa maturazione, nel corso degli anni, degli organi preposti alla prevenzione, al contrasto e alla gestione del rischio ha indotto gli attori del sistema ad agire pragmaticamente sulla base delle capacità a disposizione.

Nonostante questo, sempre in un'ottica riformatrice, queste sovrapposizioni, anche se solo parziali, potrebbero essere superate attraverso l'accorpamento dei ruoli, dei compiti e della capacità in un'unica struttura, che forse la renderebbe più lineare, anche agli occhi di operatori privati di infrastrutture critiche, imprese e cittadini. Questo organo unificato dovrebbe far convergere al suo interno le diverse anime preposte alla pubblica sicurezza, alla sicurezza nazionale e alla condivisione delle informazioni e avere nella sicurezza la sua missione principale.

Una struttura unificata probabilmente riuscirebbe a rendere meno drammatica la questione dell'allocazione delle risorse. A fronte di una minore dispersione degli attori fondamentali, sarebbe forse più semplice individuare e indirizzare chi necessita di maggiori fondi rispetto ad altri.

Le risorse che vengono fornite alle amministrazioni per la protezione cibernetica sono effettivamente ridotte rispetto a quelle dedicate in altri paesi e su questo bisognerebbe intavolare un dibattito serio. In questo dibattito **si dovrebbe partire innanzitutto dalla valutazione di alcuni fattori strutturali, delle minacce rivolte verso l'Italia**, delle vulnerabilità dei nostri sistemi e in ultimo degli obiettivi (realistici) che l'Italia vuole preporsi per la tutela dello spazio cibernetico italiano.

**Il fattore delle risorse è inevitabilmente legato con l'esigenza di disporre, nella quotidianità, di maggiore operatività a livello tecnico**. Anche in questo caso si ritiene che una razionalizzazione degli organi in un'unica struttura potrebbe sopperire inizialmente a questa carenza, salvo

poi la necessità di effettuare gli opportuni investimenti qualora la protezione cibernetica venga effettivamente ritenuta come una priorità dai decisori politici.

In ultimo, il **tema delle competenze è fondamentale** per ovvie ragioni, soprattutto in un settore fortemente tecnico come quello della sicurezza cibernetica. Conoscenza ed esperienza del settore sono indispensabili per fornire una visione di quella che deve essere la sicurezza cibernetica in Italia e il suo futuro.

**L'*expertise* è fondamentale anche per la comprensione delle questioni strutturali che suggeriscono interventi legislativi** piuttosto che altri, delle vulnerabilità che possono minare la resilienza di un sistema, oppure delle debolezze o dei fattori di forza di politiche pubbliche che vanno a strutturare la protezione dei sistemi nazionali. In questo senso è decisamente auspicabile che l'Italia si doti delle personalità giuste in grado di offrire queste competenze.

Questo non è vero solo per l'indirizzo politico e per gli aspetti manageriali della sicurezza cibernetica, ma è necessario anche **nell'operatività quotidiana**, che deve poter contare su tecnici formati secondo standard di livello internazionale. È dunque desiderabile che essi vengano preparati grazie ad un percorso d'istruzione adeguato, che forse si dovrebbe maggiormente avvicinare alla realtà operativa, ma anche attraverso un processo di formazione e aggiornamento continui una volta entrati nel mondo del lavoro.

L'OSSERVATORIO DI POLITICA INTERNAZIONALE È UN PROGETTO DI COLLABORAZIONE TRA SENATO DELLA REPUBBLICA, CAMERA DEI DEPUTATI E MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE, CON AUTOREVOLI CONTRIBUTI SCIENTIFICI.

L'OSSERVATORIO REALIZZA:

## Rapporti
Analisi di scenario, a cadenza annuale, su temi di rilievo strategico per le relazioni internazionali.

## Focus
Rassegne trimestrali di monitoraggio su aree geografiche e tematiche di interesse prioritario per la politica estera italiana.

## Approfondimenti
Studi monografici su temi complessi dell'attualità internazionale.

## Note
Brevi schede informative su temi legati all'agenda internazionale.

## Approfondimenti già pubblicati:

n. 104 L'Italia nelle missioni internazionali: problematiche operative e giuridiche (IAI – dicembre 2014)
n. 105 Traiettorie di sviluppo dei bilanci della difesa dei paesi BRICS (CeSI – gennaio 2015)
n. 106 Eserciti in miniatura? La spesa militare di Francia, Gran Bretagna e Germania al tempo della crisi (IAI – maggio 2015)
n. 107 L'Agenda di sviluppo post 2015 e l'accordo sui cambiamenti climatici (CeSPI – settembre 2015)
n. 108 Italia-America latina e il Foro italo-latinoamericano dei Parlamenti (CeSPI – settembre 2015)
n. 109 Le incognite per l'Afghanistan nel passaggio da ISAF a Resolute Support (CeSI – settembre 2015)
n. 110 Le sabbie mobili della crisi libica (CeSI – ottobre 2015)
n. 111 Rilancio della cooperazione Euro-Mediterranea (ISPI – ottobre 2015)
n. 112 Cina 2020: implicazioni globali del nuovo ciclo di riforme e prospettive per il partenariato strategico con l'Italia (T.wai – novembre 2015)
n. 113 La conferenza internazionale sul clima di Parigi. Gli impegni per l'Italia, l'Europa e il resto del mondo (CeSPI - novembre 2015)
n. 114 La sfida dei BRICS al sistema di Bretton Woods (ISPI - dicembre 2015)
n. 115 Governance economica mondiale: il ruolo dell'Italia nel G20 e nel G7 (ISPI - dicembre 2015)
n. 116 La misurazione dell'empowerment delle donne. Il dibattito sugli indicatori (CeSPI – marzo 2016)


*Coordinamento redazionale a cura della:*

**Camera dei deputati**
SERVIZIO STUDI
DIPARTIMENTO AFFARI ESTERI
Tel. 06.67604939
e-mail: st_affari_esteri@camera.it
http://www.parlamento.it/osservatoriointernazionale